

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第6057470号
(P6057470)

(45) 発行日 平成29年1月11日(2017.1.11)

(24) 登録日 平成28年12月16日(2016.12.16)

(51) Int.Cl. F I
 HO4L 12/24 (2006.01) HO4L 12/24
 HO4L 12/70 (2013.01) HO4L 12/70 I O O A

請求項の数 6 (全 8 頁)

(21) 出願番号	特願2013-157772 (P2013-157772)	(73) 特許権者	000208891
(22) 出願日	平成25年7月30日 (2013.7.30)		KDDI株式会社
(65) 公開番号	特開2015-29194 (P2015-29194A)		東京都新宿区西新宿二丁目3番2号
(43) 公開日	平成27年2月12日 (2015.2.12)	(74) 代理人	100092772
審査請求日	平成28年1月28日 (2016.1.28)		弁理士 阪本 清孝
		(74) 代理人	100119688
			弁理士 田邊 壽二
		(72) 発明者	官澤 雅典
			埼玉県ふじみ野市大原二丁目1番15号
			株式会社KDDI研究所内
		(72) 発明者	林 通秋
			埼玉県ふじみ野市大原二丁目1番15号
			株式会社KDDI研究所内
		審査官	遠水 雄太

最終頁に続く

(54) 【発明の名称】 ネットワークのアラーム処理システム

(57) 【特許請求の範囲】

【請求項1】

ネットワークのノード装置上でアラーム情報を分散処理するアラーム処理システムにおいて、

ネットワークトポロジおよび各ノード装置のIDを管理する構成管理手段と、

ノード装置により検知されたアラーム情報を蓄積するアラームDBと、

前記ネットワークトポロジに基づいて隣接装置を識別する手段と、

相互に隣接するノード装置の一方が他方のノード装置のアラームDBを参照し、前記アラーム情報と同一のアラーム情報が登録されていれば自装置のアラームDBから前記アラーム情報を削除する手段と、

アラームDBに蓄積されているアラーム情報を管理システムへ送信する手段とを具備したことを特徴とするアラーム処理システム。

【請求項2】

前記一方のノード装置は、前記他方のノード装置のアラームDBに前記アラーム情報と同一のアラーム情報が登録されていると当該アラーム情報に隣接確認フラグをセットし、前記他方のノード装置は、当該アラームを前記隣接確認フラグと共に前記管理システムへ送信することを特徴とする請求項1に記載のアラーム処理システム。

【請求項3】

前記一方のノード装置は、前記他方のノード装置のアラームDBに前記アラーム情報と同一のアラーム情報が登録されていないと当該アラーム情報にサイレントフラグをセットし

、当該アラームを前記サイレントフラグと共に前記管理システムへ送信することを特徴とする請求項 1 に記載のアラーム処理システム。

【請求項 4】

前記他方のノード装置は、アラームDBに登録されているアラーム情報に隣接確認フラグがセットされていないとサイレントフラグをセットし、当該アラームを前記サイレントフラグと共に前記管理システムへ送信することを特徴とする請求項 1 ないし 3 のいずれかに記載のアラーム処理システム。

【請求項 5】

前記相互に隣接するノード装置は、自装置に固有のIDと隣接装置に固有のIDとを比較して前記ノード装置の一方を決定することを特徴とする請求項 1 ないし 4 のいずれかに記載のアラーム処理システム。

10

【請求項 6】

前記管理システムへ送信されるアラーム情報は、SNMPトラップに記述されて送信されることを特徴とする請求項 1 ないし 5 のいずれかに記載のアラーム処理システム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ネットワークのアラーム処理システムに係り、特に、一つのアラーム原因に対して複数のノード装置から発せられるアラームを集約することで総アラーム数を減じ、かつサイレント障害を確実に検知できるネットワークのアラーム処理システムに関する。

20

【背景技術】

【0002】

ネットワーク仮想化技術の発展により、インターフェースやネットワーク自体の管理オブジェクト数が爆発的に増加し、発生するアラーム数も増加する傾向にあり、ネットワークの障害状態の把握（特に障害原因解析）に遅れが生じる課題がある。

【0003】

このような技術課題に対して、本発明の発明者等は、ネットワーク装置が保持するデータを、集中管理基盤上で管理するのではなく、ネットワーク上の各ノード装置内部にデータ処理をオフロードする手法を開発し、特許出願（特許文献 1）した。更に、トラフィック量などの品質・性能情報も同様に大幅に増加しており、管理システム側の負荷の増加が予想されるため、処理を装置へオフロードする手法を開発し、特許出願（特許文献 2）した。

30

【先行技術文献】

【特許文献】

【0004】

【特許文献 1】特願2012-030371号

【特許文献 2】特願2013-059035号

【発明の概要】

【発明が解決しようとする課題】

【0005】

40

ネットワークオペレータはネットワークサービスの異常を検知・把握するため、既存方式ではすべての装置で設定されたSNMP（Simple Network Management Protocol）やSyslog情報を、外部管理システム（NMS：Network Management System）で受信し、状態遷移の把握を行っている。しかしながら、既存方式では装置単位でアラーム情報が送信されるため、直接原因でないアラームが送出されてくるとともに、管理対象となるノード装置数が増えるとアラーム情報が爆発的に増加し、結果的に処理遅延が生じる。さらに、サイレント障害の発見に遅延が生じうる。

【0006】

本発明の目的は、上記の技術課題を解決し、管理システムが持つアラーム管理機能の一部をネットワーク上の各ノード装置内部に配備して機能を分散化すると共に、隣接するノ

50

ード装置同志がアラーム情報を確認することにより、管理システムへ通知するアラーム数を削減し、更にはサイレント障害を検知できるアラーム処理システムを提供することにある。

【課題を解決するための手段】

【0007】

上記の目的を達成するために、本発明は、ネットワークのノード装置上でアラーム情報を分散処理するアラーム処理システムにおいて、以下の構成を発明特定事項とした点に特徴がある。

【0008】

(1) ネットワークトポロジおよび各ノード装置のIDを管理する構成管理手段と、ノード装置により検知されたアラーム情報を蓄積するアラームDBと、ネットワークトポロジに基づいて隣接装置を識別する手段と、相互に隣接するノード装置の一方が他方のアラームDBを参照し、前記アラーム情報と同一のアラーム情報が登録されていれば自装置のアラームDBから前記アラーム情報を削除する手段と、アラームDBに蓄積されているアラーム情報を前記管理システムへ送信する手段とを具備した。

【0009】

(2) 一方のノード装置は、他方のノード装置のアラームDBにアラーム情報と同一のアラーム情報が登録されていると当該アラーム情報に隣接確認フラグをセットし、他方のノード装置は、当該アラームを隣接確認フラグと共に前記管理システムへ送信するようにした。

【0010】

(3) 一方のノード装置は、他方のノード装置のアラームDBにアラーム情報と同一のアラーム情報が登録されていないと当該アラーム情報にサイレントフラグをセットし、当該アラームを前記サイレントフラグと共に管理システムへ送信するようにした。

【0011】

(4) 他方のノード装置は、アラームDBに登録されているアラーム情報に隣接確認フラグがセットされていないとサイレントフラグをセットし、当該アラームを前記サイレントフラグと共に管理システムへ送信するようにした。

【発明の効果】

【0012】

本発明によれば、以下のような効果が達成される。

(1) 同一のネットワーク障害に起因した同一アラームが複数のノード装置において検知されても、隣接ノード同士で同一アラームが一方の隣接ノードへ集約されるので、複数のノード装置から同一アラームがそれぞれ管理システムへ送信される不都合が防止される。

【0013】

(2) 自装置のみに登録されて隣接ノード装置には未登録のアラームをサイレント障害に起因したアラームと推定し、当該アラームがサイレント障害に起因したアラームである旨の情報と共に管理システムへ送信されるので、管理システムはサイレント障害を簡単に判別できるようになる。

【図面の簡単な説明】

【0014】

【図1】本発明に係るアラーム処理システムが適用されるネットワークノード装置の構成を示した機能ブロック図である。

【図2】発明の一実施形態の動作を模式的に表現した図である。

【図3】本発明の一実施形態の動作を示したフローチャートである。

【図4】アラーム通知のフォーマットを示した図である。

【発明を実施するための形態】

【0015】

以下、図面を参照して本発明の実施の形態について詳細に説明する。図1は、本発明に係るアラーム処理システムが適用されるネットワークノード装置の構成を示した機能プロ

10

20

30

40

50

ック図であり、ネットワーク上には多数のネットワークノード装置INMおよびその管理システム1が配置されている。

【0016】

各ノード装置INMではSNMPエージェントがそれぞれ稼働し、各SNMPエージェントは、あらかじめ指定されたイベントの発生や、プロセス値の閾値越え等が検知されるとSNMPトラップ(Trap)を送出する。当該SNMPトラップは、各ノード装置INMのAPIを経由して、管理システム1のSNMPマネージャへ送信される。

【0017】

ノード装置INMにおいて、アラーム処理基盤21は、SNMPエージェントが送出的るSNMPトラップをリアルタイムにモニタリングし、本基盤上に設定されたアラームマスクルールに基づいてマスク処理を行う。アラームマスクルールとは、高速データ処理基盤上に設定されたフィルタ機能により、不必要と判断されたアラームをマスクする機能であり、隣接装置間のアラーム受信状況を確認するアラーム処理フロー機能も具備する。

10

【0018】

本実施形態では、構成管理DBで管理されているConnectionおよびConnectionLess、ならびにネットワークで保持されるOID情報以外がマスクされる。そして、アラームマスクされたアラームがアラーム保存DB23で一定時間保存される一方、アラームマスクされなかったアラームはアラームDB22へ保存される。共有データベース25は、複数のノード装置間で構成管理データ(装置構成情報やネットワークポロジ情報)を共有管理する仕組みを提供する。

20

【0019】

API(外部インターフェース機能部)は、アラーム情報の記述されたSNMPトラップを管理システム1へ転送するインターフェース機能を実現する。共有DB25には、ネットワークポロジおよび各ノード装置INMに固有の識別IDが登録されている。本実施形態では、各ノード装置INMの識別IDとしてIPアドレスが用いられる。

【0020】

次いで、図2のブロック図および図3のフローチャートを参照して本発明の動作について詳細に説明する。

【0021】

ステップS1では、各ノード装置INMにおいて稼働中のSNMPエージェントから送出的たアラーム(Trap)が受信されたか否かが判定される。ここでは、相互に隣接するノード装置INM1, INM2において、同一のネットワーク障害に起因した同一アラームの記述されたTrapが、ほぼ同時刻に受信されたものとして説明を続ける。

30

【0022】

ステップS2では、当該アラームが各ノード装置INM1, INM2において自装置のアラームDB22にそれぞれ登録される。本実施形態では、図2に示したように、アラームの受信時刻およびその送信元(source)情報、ならびにSNMPトラップのOID(オブジェクトID)に記述されているアラーム(Alarm)情報が抽出されてアラームDB22の同一レコードに登録される。

【0023】

ステップS3では、構成管理DB25に登録されているネットワークポロジに基づいて隣接ノード装置INMが識別され、当該隣接ノード装置の識別ID(本実施形態では、IPアドレス)が前記登録されたアラームのレコードに隣接情報として登録される。すなわち、ノード装置INM1では、隣接装置としてノード装置INM2が認識されるので、そのIPアドレスがアラームDB22の対応レコードに隣接情報として登録される。ノード装置INM2では、隣接装置としてノード装置INM1が認識されるので、そのIPアドレスがアラームDB22の対応レコードに隣接情報として登録される。

40

【0024】

ステップS4では、各ノード装置INM1, INM2において自装置のアラームDB22が参照され、自装置の装置ID(source情報)および隣接装置の装置ID(隣接情報)のいずれが相対的に

50

若番であるか判断される。ここでは、ノード装置INM1の装置ID(ノード1)よりもノード装置INM2の装置ID(ノード2)が若番であるものとして説明を続ける。したがって、ノード装置INM1では処理がステップS4からステップS5へ進み、ノード装置INM2では処理がステップS4からステップS12へ進む。

【0025】

初めに老番のノード装置INM1の動作に注目し、ステップS5, S6では、隣接するノード装置INM2のアラームDB22への接続が試行され、接続できればステップS7へ進む。ステップS7では、ノード装置INM2のアラームDB22に、前記ステップS1で自装置が受信したアラーム(アラーム1)と同一のアラームが重複登録されているか否かが判定される。ここでは、アラーム1が重複登録されていると判定されるのでステップS10へ進み、当該隣接するノード装置INM2のアラームDB22において、前記アラーム1と対応付けられた同一レコードの隣接確認フラグFnがセット(=1)される。ステップS11では、ノード装置INM1のアラームDB22から前記重複登録されていたアラーム1が削除される。

10

【0026】

次いで若番のノード装置INM2の動作に注目し、ステップS12では所定の時間だけ待機する。ステップS13では、自装置INM2のアラームDB22に既登録のアラームについて、その隣接確認フラグFnが「1」であるか否かが判定され、隣接確認フラグFnが「1」であればステップS9へ進み、「1」でなければステップS8へ進む。本実施形態では、前記ステップS10においてアラーム1の隣接確認フラグFnがセットされているのでステップS9へ進む。ステップS9では、前記アラーム1の記述されたSNMPトラップが管理システム1へ送出される。

20

【0027】

これに対して、ノード装置INM1にサイレント障害が発生し、そのアラーム(アラーム2)の記述されたTrapがノード装置INM1のみで受信されていれば、当該処理はノード装置INM1のみで実行され、そのステップS7では、同一アラームが隣接するノード装置INM2のアラームDB22には未登録と判定されるのでステップS8へ進む。ステップS8では、自装置INM1のアラームDB22において前記アラーム2と対応付けられたサイレントフラグFsがセットされる。ステップS9では、前記アラーム2の記述されたSNMPトラップが管理システム1へ送出される。

30

【0028】

図4は、各ノード装置INMから管理システム1へ送信されるSNMPトラップのフォーマットを示した図であり、本実施形態では、OID(オブジェクトID)に拡張領域として「対向装置情報」および「サイレント故障情報」が用意されている。そして、前記ステップS8においてサイレントフラグFsがセットされると、ステップS9では、「元のアラーム情報」として前記アラーム2が記述され、「対向装置情報」としてsource情報が記述され、「サイレント故障情報」として前記サイレントフラグFsの値(ここでは、1)の記述されたSNMPトラップが生成されて管理システム1へ送出される。

40

【0029】

管理システム1では、SNMPトラップを受信した際に、そのOIDの「サイレント故障情報」がセット(=1)されていれば、「対向装置情報」に記述されたノード装置INMにおいてサイレント障害が発生していると認識できる。また、「サイレント故障情報」がセットされていない場合は、サイレント障害以外の例えばリンク障害が発生していると判断できる。

【0030】

なお、上記の実施形態では、ネットワーク機器を監視、制御するための通信プロトコルとしてSNMPを利用するものとして説明したが、本発明はこれのみに限定されるものではなく、各ノード装置において検知された障害にオリジナルのメッセージやフラグを記述して管理システムに通知できるのであれば、他のプロトコルを用いても良い。

【0031】

本実施形態によれば、同一のネットワーク障害に起因した同一アラームが複数のノード装置INMにおいて重複検知されても、隣接ノード同士で同一アラームが一方の隣接ノード

50

へ集約されるので、複数のノード装置INMから同一アラームがそれぞれ管理システム1へ送信される不都合が防止される。

【0032】

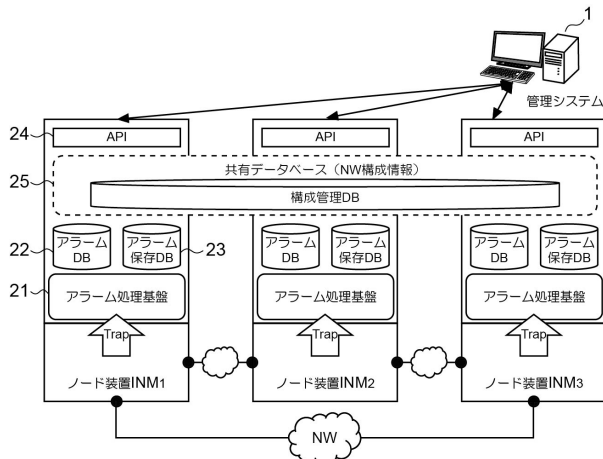
また、本実施形態によれば、自装置のみに登録されて隣接ノード装置には未登録のアラームをサイレント障害に起因したアラームと推定し、当該アラームがサイレント障害に起因したアラームである旨の情報と共に管理システム1へ送信されるので、管理システム1はサイレント障害を簡単に判別できるようになる。

【符号の説明】

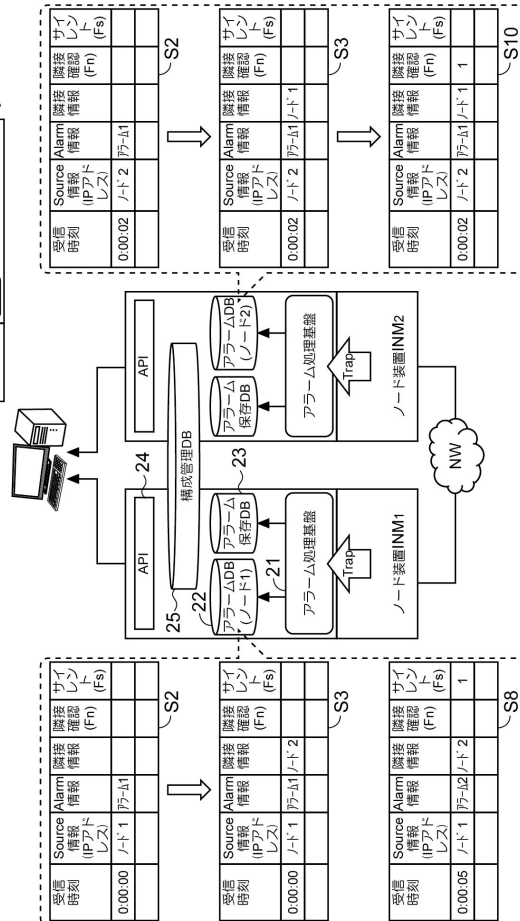
【0033】

1 ... 管理システム, 21 ... アラーム処理基盤, 22 ... アラームDB, 23 ... アラーム保存DB, 24 ... API, 25 ... 共有データベース

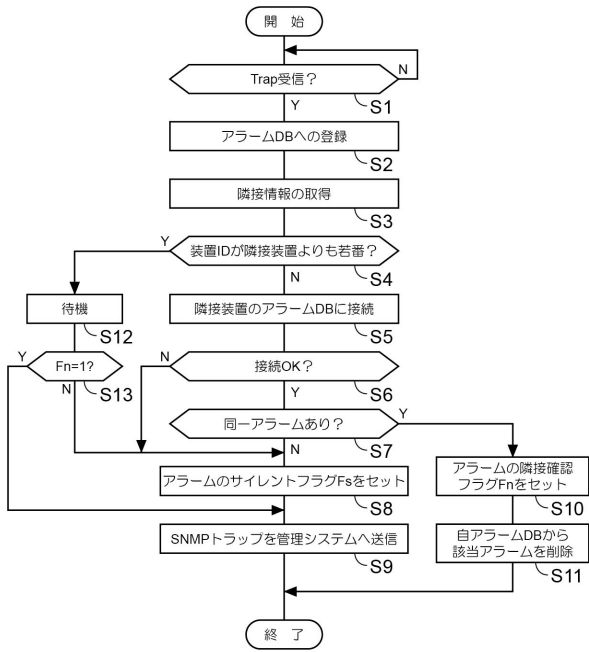
【図1】



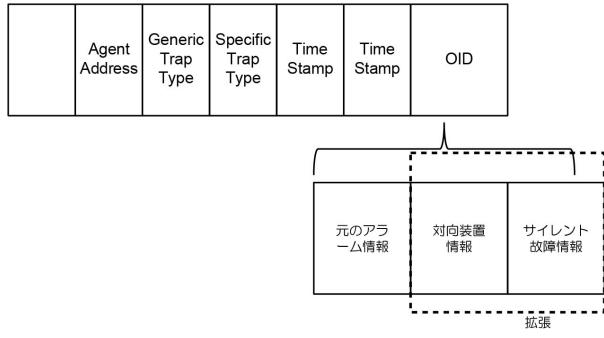
【図2】



【図3】



【図4】



フロントページの続き

(56)参考文献 米国特許出願公開第2008/0284581 (US, A1)

特開2009-296320 (JP, A)

特開2002-158673 (JP, A)

特開平07-264212 (JP, A)

(58)調査した分野(Int.Cl., DB名)

H04L 12/24

H04L 12/70